AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method of protecting a data center against a denial of service attack, the method ~~comprises~~comprising:

sending queries to data collectors, deployed at different points in a network that carries network traffic to the data center, the data collectors collect statistical information on network packets sent over the network, the queries to request the statistical information from at least some of the data collectors; and

sending the statistical information from the data collectors in response to the queries; and

processing the statistical information to determine the source of suspicious network traffic sent to the data center~~.~~ by aggregating statistical information of traffic flows from a source address and source port to a destination address and destination port, measured over different periods of time.

2. (Previously presented) The method of claim 1 wherein the network packets from the attacker have faked, random source addresses that change with time, and sending queries further comprises:

sending queries to the data collectors for the statistical information based on victim destination address for the data center.

3. (Previously presented) The method of claim 1 wherein processing further comprises:

determining, from at least in part, the collected statistical information, what data centers are involved in the attack on the victim data center.

4. (Previously presented) The method of claim 3 wherein determining is performed by a control center that receives the statistical information from the data collectors, and determining further comprises:

sending data to/from a gateway device that is associated with the victim data center.

5. (Previously presented) The method of claim 4 wherein the gateway identifies the network address of the data center victim, via a message to the control center.

6. (Previously Presented) The method of claim 1 wherein the queries and the statistical information are sent over a redundant network that does not carry the packet traffic to deliver collected statistical information to a central control center in response to the queries sent from the central control center.

7. (Original) The method of claim 5 wherein message indicates the type of attack.

8. (Previously Presented) The method of claim 1 wherein a source of the attack is behind a gateway.

9. (Previously Presented) The method of claim 8 wherein if a source of the attack is behind a gateway, the control center issues a request to the gateway that the attacking system is behind to prevent the attacking traffic from attacking system from reaching the network.

10. (Previously presented) The method of claim 8 wherein if a source of the attack is behind a gateway, the gateway that the attacking system is behind selectively discards traffic that appears to be malicious traffic and that contains the victim destination address of the data center.

11. (Currently amended) The method of claim 1 wherein if a source of the attack is not behind a gateway, ~~the control~~a control center queries the data collectors to provide information about possible locations of the attacking system.

12. (Currently amended) The method of claim 1 wherein if a source of the attack is not behind a gateway, the method further comprises:

contacting administrators at locations involved in the attack to have the administrators take action to filter out packets with ~~the destination~~a destination address.

13. (Previously presented) The method of claim 1 wherein the attack is a low-grade spoofing-type of attack that does not compromise network traffic flow between the victim data center and Internet.

14. (Previously presented) The method of claim 1 wherein the attack is a high-grade attack that compromises network traffic flow between the victim data center and Internet.

15. (Currently amended) A method of protecting a victim data center against a denial of service attack, the method ~~comprises~~comprising:

receiving packets with faked, random source addresses;

receiving, from a gateway disposed near the victim data center, a notification that the victim data center is under an attack;

sending queries to data collectors deployed at different points in a network that carries network traffic to the victim data center, the data collectors to sample network packets and collect statistical information on network packets sent over the network, the queries being requests for statistical information from data collectors that have examined network traffic with ~~the victim~~a victim destination address; and

determining ~~the data~~a data center or centers involved in the attack on the victim data center by analyzing collected statistical information from the data ~~collectors.~~collectors, wherein the analyzing comprises aggregating statistical information of traffic flows from a source address and source port to a destination address and destination port, measured over different periods of time.

16. (Currently amended) The method of claim 15 further comprising:

communicating statistical information from ~~the control~~a control center to/from a gateway device that is disposed with the victim data center.

17. (Previously Presented) The method of claim 16 wherein if a source of the attack is behind a gateway, the control center issues a request to the gateway to block the attacking traffic.

18. (Previously Presented) The method of claim 17 wherein if a source of the attack is behind a gateway, the gateway selectively discards traffic that appears to be malicious traffic and that contains the victim destination address.

19. (Currently amended) The method of claim 15 wherein if a source of the attack is not behind a gateway, the method comprises:

contacting administrators at locations involved in attack to filter out packets having ~~the destination~~a destination address.

20. (Currently amended) A system to thwart denial of service attacks on a victim data center, the system comprising:

a plurality of data collectors monitors dispersed throughout a network, the data collectors monitors collecting statistical data on network traffic;

a control center coupled to the plurality of data collectors, the control center, comprising

a memory;

a processor; and

executing a computer readable medium storing a computer program product, the stored on a computer readable medium, comprising instructions for causing the control center a computer to:

receive from the data center victim site a notification that the victim data center is under an attack; and in response to receiving the notification,

send queries to data collectors to request the statistical information from collected by the data collectors based on network traffic, the statistical information used to determine ~~a the source~~a source of suspicious network traffic being sent to the data center ~~victim;~~victim, wherein determining the source of suspicious network traffic comprises aggregating statistical information of traffic flows from a source address and source port to a destination address and destination port, measured over different periods of time;

a gateway device that passes network packets between the network and the victim data center, the gateway disposed to protect the victim data center, and being coupled to the control center.

21. (Previously Presented) The system of claim 20 wherein the data collectors collect statistical information on network packets that pass through points in the network that the data collectors monitor.

22. (Previously presented) The system of claim 20 wherein the control center further comprises instructions to:

determine a source of the attack on the victim data center by analyzing collected statistical information from the data collectors.

23. (Previously presented) The system of claim 20 wherein the control center and gateway device associated with the victim data center exchange data including statistical information to thwart the attack.

24. (Previously presented) The system of claim 20 wherein data exchanged between the control center and gateway device associated with the victim data center are sent over a redundant network that is a different network than the network that is being monitored by the data collectors.

25. (Previously Presented) The system of claim 20 wherein if the control center determines that the source of the attack is behind a gateway, the control center issues a request to the gateway that the source of the attack is behind to block the attacking traffic.

26. (Previously presented) The system of claim 20 wherein if the control center determines that the source of the attack is behind a gateway, the control center issues a request to the gateway to selectively discard traffic that contains a the victim destination address for the data center.

27. (Previously Presented) The system of claim 20 wherein if the source of the attack is not behind a gateway, the control center queries the data collectors to provide information about possible locations of the source of the attack.

28. (Previously presented) The system of claim 27 wherein if the source of the attack is not behind a gateway, the system includes instructions to contact administrators at locations involved in attack to have the administrators cause filters to be installed in the data center take action to filter out packets with the victim destination address.

29. (Currently amended) A computer program product residing on a computer readable media for protecting a victim data center against a denial of service attack, the computer program product, comprising instructions for causing a computing device to:

receive a notification that the victim data center is under an attack;

send queries to data collectors deployed at different points in a network that carries network traffic to the victim data center, the data collectors to sample network traffic and collect statistical information on packets sent over the network, the queries to request statistical information from data collectors that have examined network traffic with the victim destination address; and

determine a source of the attack on the victim data center by analyzing collected information from the data ~~collectors.~~collectors, wherein the analyzing comprises aggregating statistical information of traffic flows from a source address and source port to a destination address and destination port, measured over different periods of time.

30. (Previously Presented) The computer program product of claim 29 further comprising instructions to:

send data including statistical information between a gateway device that is disposed with the victim data center and a control center.

31. (Previously Presented) The computer program product of claim 29 further comprising instructions to:

determine whether the source of the attack is behind a gateway and if the source of the attack is behind a gateway,

issue a request to the gateway to block the attacking traffic.

32. (Previously Presented) The computer program product of claim 29 further comprising instructions to:

determine whether the source of the attack is behind a gateway and if the source of the attack is not behind a gateway,

send a message to contact administrators at locations involved in the attack to filter out packets having the destination address.

33. (Previously Presented) The method of claim 1 further comprising:

receiving from the victim site a notification that the victim site is under an attack.